113
*
, 12 m
99
100

IN THE UNITED STATES PATE Applicant(s): Zimmermann	ENT AND TRADEMARK OFFICE
Approant(s). Zimmermann	
Application No.: Unassigned	
Filed: June 21, 2001	Group Art Unit: Unassigned
Title: Cryptographic System with Methods for User-Controlled Message Recovery	Examiner: Unassigned
Attorney Docket No.: 002.0218.01	
Box Patent Application Assistant Commissioner for Patents Washington, D.C. 20231	
DRAWING TRANS	MITTAL LETTER
Sir:	
Enclosed herewith please find:	
() sheets of redlined drawing(drawing(s). Upon approval of be submitted.	(s) which indicate proposed changes to the these proposed changes, formal drawing(s) will
sheets of corrected formal dr Drawings Objection (PTO-948	rawing(s), as required by the Notice of Patent 8) which accompanied the Office Action dated
sheets of corrected formal dr Drawing(s) Objection (PTO-9) dated	rawing(s), as required by the Notice of Patent 48) and approved in the Notice of Allowability
(X) 14 sheets of formal drawings, shapplication.	submitted with the enclosed Utility Patent
Examiner's approval of the entry of these drawing been added.	gs is respectfully requested. No new matter has
	Respectfully Submitted,

The Law Offices of Patrick J.S. Inouye 810 3rd Avenue, Suite 258 Seattle, Washington 98104

Attorney/Agent for Applicant(s) Reg. No. 40297

Date: June 21, 2001

Figure 1A. (Prior Art)

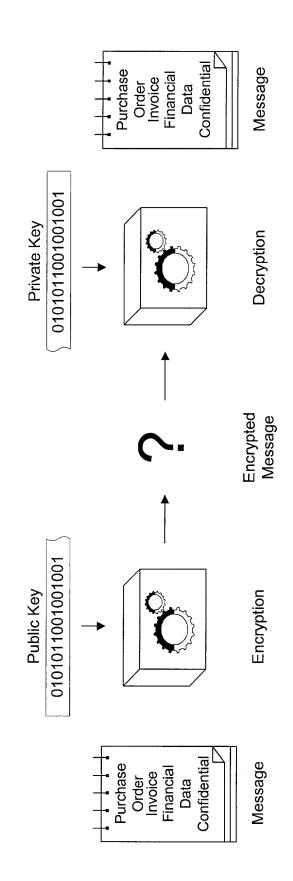


Figure 1B. (Prior Art)

	Recipient's	ent's	Sender's	der's
	Private Key	Public Key	Private Key	Public Key
Sender Encrypts with:		×		
Sender Signs with:			×	
Recipient Decrypts with:	×			
Recipient Verifies Signature with:				×

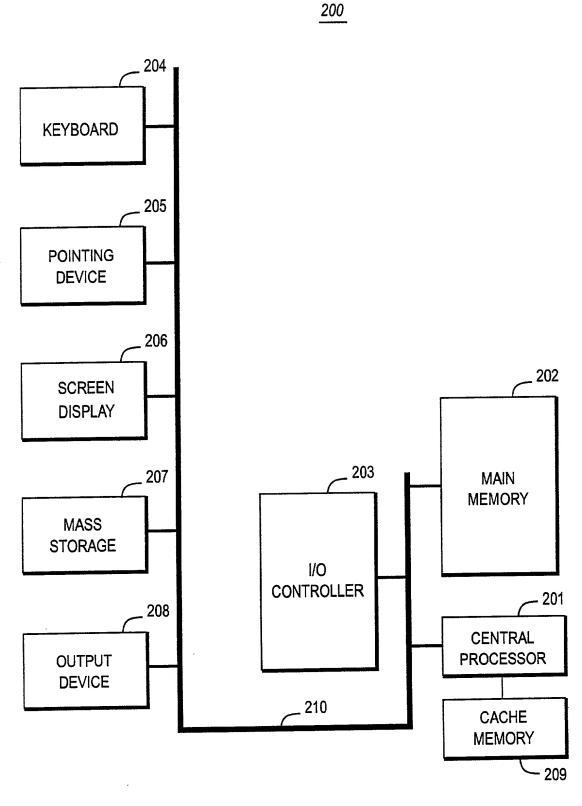


FIG. 2



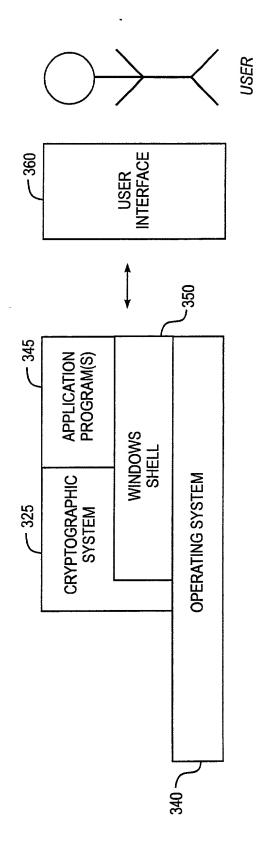
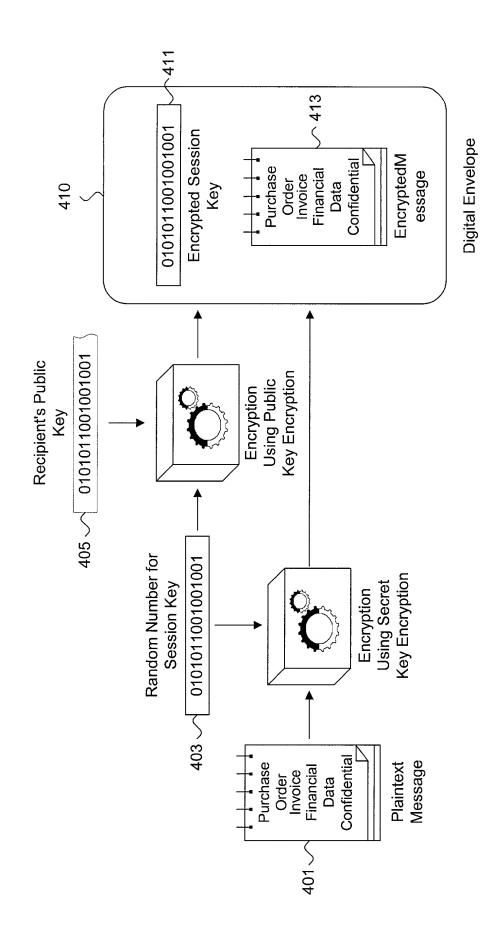


FIG. 3

Figure 4.



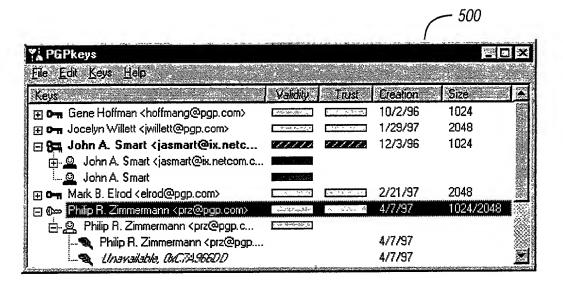


FIG. 5A

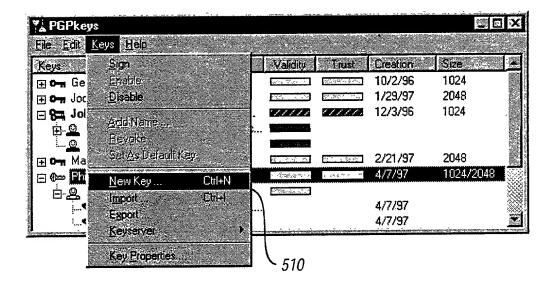


FIG. 5B

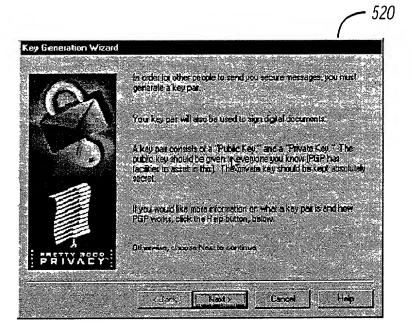


FIG. 5C

ieneration Wizar	The second secon
	What name and small address should be associated with this key pair?
	By being your name and small address here, you let your correspondents know that the key they are daing belongs to you.
	Full marks
	Email address
RIVACY	

FIG. 5D

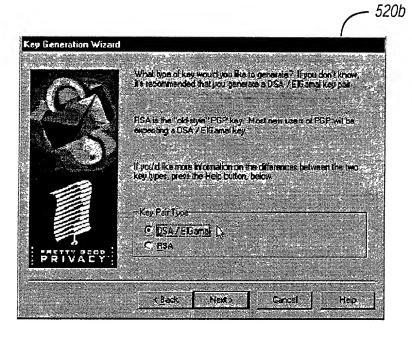


FIG. 5E

7	How large a key pair do you with to generate? As a n.le. larger keys are more secure. But slower
F/T	For most applications, 1024, 2046 bit keys are quite sufficient.
	- Key Pau Spe
	€ 768 lites
3/2	C 1024 bis
	C 1536 bits (1024 DSA/1536 f(Samal)
	© 2048 bits (1024 DSA/2048 ElGanal)
	C 3072 bits (2048 DSA/3072 ElGame)
	Custom (512 - 4096 bits)
RIVACY	

FIG. 5F

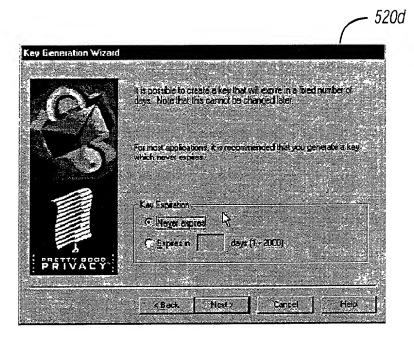


FIG. 5G

S A	Your private key will be protected by a passphrase. It is important that you do not write this passphrase down, so it needs to be easy. It remember. We recommend that your passphrase be at least eight characters.
	long and contain at least one non-algraphetic character.
	l⊽'Hide⊤ypeng Passphrese
	Passpirase Confirmation
FIVER.	

FIG. 5H

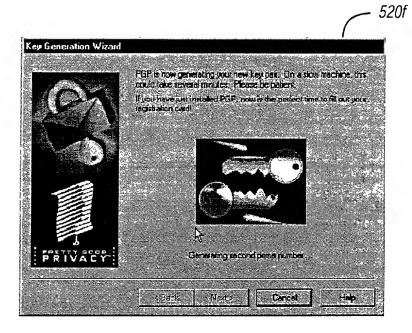


FIG. 51

Generation Wiza	rd ·	
7.3	You have an old private key on your k and small address as the key you've p	
	We recommend that you now sign you to do so, simply enter the passiphrase field below.	
	If you do not wish to sign you new key uncheck "Sign my new key now," and arways sign your now key at a later da	press 'Next' You can
	Sign my new key mow	
	Old Private Key <u>P</u> assphrace	I Hide Typing
PRIVATER		

FIG. 5J

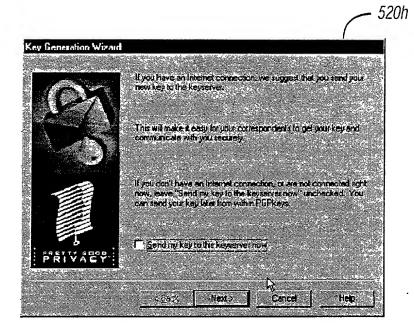


FIG. 5K

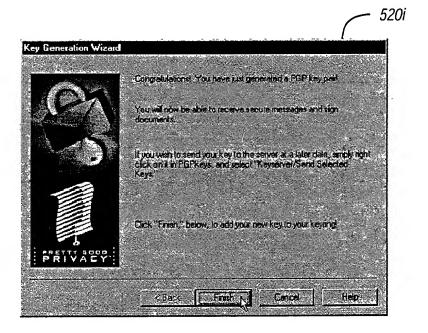


FIG. 5L

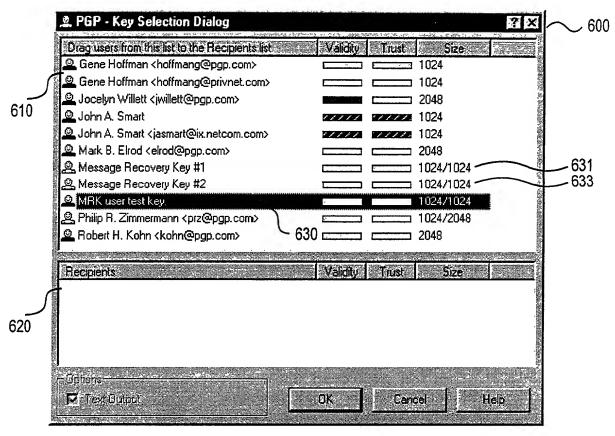


FIG. 6A

PGP - Key Selection Dialog	a manada sakat sakat ka ka ka manada katabatan da kataba ka	enenga etter var og se
Drag users from this list to the Recipients list	Validity Trust	Size
Gene Hoffman <hoffmang@pgp.com></hoffmang@pgp.com>	e 1	024
Gene Hoffman <hoffmang@privnet.com></hoffmang@privnet.com>		024
Jocelyn Willett <jwillett@pgp.com></jwillett@pgp.com>		048
🚇 John A. Smart	17777 17777	024
John A. Smart < jasmart@ix.netcom.com>		024
Mark B. Elrod ⟨elrod@pgp.com⟩		048
🚇 Message Recovery Key #1		024/1024
🚇 Message Recovery Key #2		024/1024
MRK user test key		024/1024
A Philip R. Zimmermann <prz@pgp.com></prz@pgp.com>		024/2048
Robert H. Kohn <kohn@pgp.com></kohn@pgp.com>		048
Recipients:	Validity Trust	Size: 1
		1 024/1024
-	630a	₽.
- Options-		
▼ TextOutpot	OK Cance	d Help

FIG. 6B

PGP - Key Selection Dialog	¶×.
Drag users from this list to the Recipients list	Validity Trust Size
Gene Hoffman <hoffmang@pgp.com></hoffmang@pgp.com>	
Gene Hoffman <hoffmang@privnet.com></hoffmang@privnet.com>	1024
Jocelyn Willett ⟨¡willett@pgp.com⟩	2048
🕰 John A. Smart	1024
John A. Smart <jasmart@ix.netcom.com></jasmart@ix.netcom.com>	2222 2222 1024
Mark B. Elrod <elrod@pgp.com></elrod@pgp.com>	2048
Philip R. Zimmermann <prz@pgp.com></prz@pgp.com>	1024/2048
☐ Robert H. Kohn <kohn@pgp.com></kohn@pgp.com>	2048
Recipients Message Recovery Key #1 Message Recovery Key #2	Validīty Trust Size 1024/1024
A MRK user test key Options	1024/1024
▼ Text Output	OK Cancel Help

FIG. 6C

PGP - Key Selection Dialog	2 X	
Drag users from this list to the Recipients list	Validity Trust Size	
Gene Hoffman <hoffmang@pgp.com></hoffmang@pgp.com>	1024	
Gene Hoffman <hoffmang@privnet.com></hoffmang@privnet.com>	1024	
Jocelyn Willett <jwillett@pgp.com></jwillett@pgp.com>	2048	
🚨 John A. Smart	1024	
Dohn A. Smart < jasmart@ix.netcom.com	2000 2000 1024	
Mark B. Elrod <elrod@pgp.com></elrod@pgp.com>	2048	
Philip R. Zimmermann <prz@pgp.com></prz@pgp.com>	1024/2048	
Robert H. Kohn <kohn@pgp.com></kohn@pgp.com>	2048	
Recipients	Validitu Trust Size	
🚇 Message Recovery Key #1	1024/1024	
. Message Recovery Key #2	1024/1024	$\frac{1}{1}$ 63
의 MRK user test key	1024/1024	
Öptións. V Text Guitput	DK Cancel Help:	

FIG. 6D

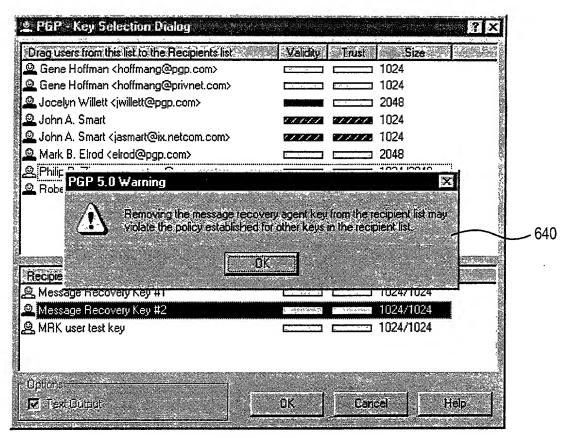


FIG. 6E

🚨 PGP - Key Selection Dialog				3[X]
Drag users from this list to the Recipients list	Validity T	tust	Size	
🙎 Gene Hoffman <hoffmang@pgp.com></hoffmang@pgp.com>		1	024	
🙎 Gene Hoffman <hoffmang@privnet.com></hoffmang@privnet.com>	. A A . A . A		024	
Jocelyn Willett <jwillett@pgp.com></jwillett@pgp.com>		2	048	
👱 John A. Smart	11111 11	446	024	
John A. Smart <jasmart@ix.netcom.com></jasmart@ix.netcom.com>	01111 V	1111	024	
Mark B. Eirod ⟨eirod@pgp.com⟩	V	2	048	
🙎 Message Recovery Key #2		1	024/1024	
2 Philip R. Zimmermann <prz@pgp.com></prz@pgp.com>			024/2048]
Robert H. Kohn <kohn@pgp.com></kohn@pgp.com>		2	048	
1				
Recipients	Validity T	rust	5ize	
Message Recovery Key #1			024/1024	
MRK user test key		1	024/1024	
				•
1 ************************************				
Options		4	-1	an result
▼ Text Bulput:	DK	Cance		Help

FIG. 6F

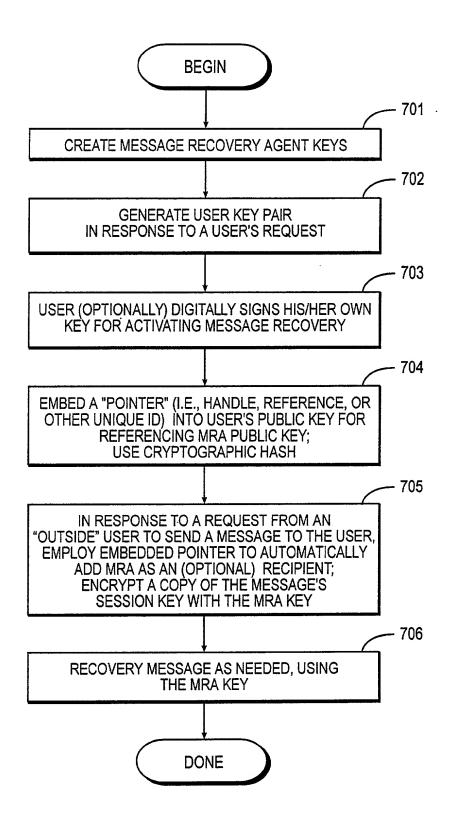


FIG. 7